CLMPTO

Michelle R. Eason

1. A method of authenticating communications, the method comprising:

using a mobile communications device, which includes a cryptographic module for use in mobile communication, as an authentication token.

2. A method of authenticating communications as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

3. (Amended) A method of authenticating communications as claimed in claim 1, wherein the use of the mobile communications device as an authentication token includes using public key encryption of communications.

4. (Amended) A method of authenticating communications as claimed in claim 1, wherein the mobile communications device uses the cryptographic module for Wireless Transport Layer Security communications.

5. (Amended) A method of authenticating communications as claimed in claim 1, wherein the mobile communications device is used as an authentication token for a computer, and authenticates communications between the computer and an authentication server.

6. A method of authenticating communications as claimed in claim 5, comprising providing a wired connection between the mobile communications device and the computer.

7. A method of authenticating communications as claimed in claim 5, comprising providing a wireless connection between the mobile communications device and the computer.

8. A mobile communications device, comprising a cryptographic module, the cryptographic module being usable:

(a) for encoding wireless communications from the device;

(b) for authenticating a user of the device towards an authentication server.

9. A mobile communications device as claimed in claim 8, the cryptographic module being usable for authenticating a user of a separate computer towards the authentication server.

10. A mobile communications device as claimed in claim 9, having a short-range wireless communications transceiver, for sending signals to and receiving signals from the computer.

11. A mobile communications device as claimed in claim 10, wherein the short-range wireless communications transceiver uses Bluetooth wireless technology.

12. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security.

13. (Amended) A mobile communications device as claimed in claim 8, having means for allowing biometric identification of a user.

14. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module uses public key cryptography.

15. (Amended) A mobile communications device as claimed in claim 8, comprising means for sending and transmitting data using WAP.

16. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module is realized in hardware in the device.

17. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module is realized in software in the device.

18. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module is provided on an external smart card.

19. (Amended) A mobile communications device as claimed in claim 8, wherein the cryptographic module comprises a Wireless Identity Module (WIM) card.

20. A mobile communications device as claimed in claim 19, wherein the cryptographic module comprises a Wireless Identity Module (WIM) card which allows communications using Wireless Transport Layer Security.

21. A WAP-enabled mobile communications device, which is capable of use as an authentication token.

22. A communications network, comprising:

at least one WAP gateway, which is enabled to encrypt communications on the basis of Wireless Transport Layer Security;

at least one authentication server operable in a first authentication protocol; and

a WAP-enabled client device, including a cryptographic module, the cryptographic module being usable for encrypting communications with the WAP gateway using Wireless Transport Layer Security, and the cryptographic module being further usable as an authentication token for authenticating a user of the device towards the authentication server, using the first authentication protocol.

23. A network as claimed in claim 22, wherein the cryptographic module is realised in hardware in the client device.

24. A network as claimed in claim 22, wherein the cryptographic module is realised in software in the client device.

25. A network as claimed in claim 22, wherein the cryptographic module is provided on an external smart card.

26. A network as claimed in claim 22, wherein the cryptographic module comprises a Wireless Identity Module (WIM) card.

27. (Amended) A network as claimed in claim 22, comprising a computer, the client device having a connection to the computer such that it acts as an authentication token therefor.